EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

July 12, 2016

M-16-15

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director
Office of Management and Budget

Beth F. Cobert
Acting Director
Office of Personnel Management

Tony Scott
Federal Chief Information Officer
Office of Management and Budget

SUBJECT: Federal Cybersecurity Workforce Strategy

Executive Summary

Every day, Federal departments and agencies face increasingly sophisticated and persistent cyber threats that pose strategic, economic, and security challenges to our Nation. These cyber threats demonstrate the need for critical security tools, and equally as important, the need to employ the Federal civilian cybersecurity workforce with the necessary knowledge, skills, and abilities to use those tools to enhance the security of the Federal digital infrastructure and improve the ability to detect and respond to cyber incidents when they occur. Both Federal and private sector executives cite the lack of professionals with the requisite knowledge and skills as a significant impediment to improving their cybersecurity. However, there simply is not a sufficient supply of cybersecurity talent to meet the increasing demand of the Federal Government. Recent industry reports project this shortfall will expand rapidly over the coming years unless companies and the Federal Government act to expand the cybersecurity workforce to meet the increasing demand for talent.

To develop and strengthen the workforce of Federal cybersecurity professionals, the Government must demonstrate that it is the employer of choice for such professionals, as it offers rewarding,

unique, and dynamic careers that rival opportunities anywhere else in the world. In particular, the Federal cybersecurity workforce is entrusted with the mission of protecting government information technology (IT) systems, networks, and data from the most sophisticated adversaries; safeguarding sensitive data; supporting our Nation's financial systems; and securing our critical infrastructure, and intelligence systems. The Government is seeking college students and industry employees of all skill and experience levels to bring their skills into public service to take on these challenging missions and further expand the existing, highly capable Federal cybersecurity workforce. Moreover, the Government seeks to provide cybersecurity professionals the flexibility to join Federal service at different times in their careers to create new opportunities for career growth, development, and innovation for such professionals across private industry, academia, and Government.

This Federal Cybersecurity Workforce Strategy (the Strategy) details government-wide actions to identify, expand, recruit, develop, retain, and sustain a capable and competent workforce in key functional areas to address complex and ever-evolving cyber threats. Most importantly, the Strategy presents new approaches to address persistent Federal workforce challenges. The Strategy anticipates that the Government will see the return on its investment through enhancements to Federal cybersecurity and the improved knowledge, skills, and abilities incoming cybersecurity talent bring to the Federal workforce.

Introduction

Addressing the Nation's growing challenges requires a capable Federal cybersecurity workforce that possesses the necessary cybersecurity knowledge, skills, and competencies to counter increasingly sophisticated and ever-changing threats. The Federal Government, however, faces a cybersecurity workforce shortage due to persistent recruitment, hiring, and retention challenges, and increasing competition with private sector companies for top talent.

The Federal Government must take immediate and broad-sweeping actions to address the growing workforce shortage and establish a pipeline of well-qualified cybersecurity talent. To this end, in June of 2015, the Office of Management and Budget (OMB) launched the Cybersecurity Sprint to rapidly improve cybersecurity across the Federal Government. The Cybersecurity Sprint included a review of Federal cybersecurity policies, plans, and procedures, which revealed two key observations about the Federal cybersecurity workforce:

1. The vast majority of Federal agencies cite a lack of cybersecurity and IT talent as a major resource constraint that impacts their ability to protect information and assets; and,
2. There are a number of existing Federal initiatives to address this challenge, but implementation and awareness of these programs are inconsistent.

Accordingly, OMB issued the *OMB Memorandum M-16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government"* on October 30, 2015. The CSIP called for OMB and the Office of Personnel Management (OPM) to publish a Cybersecurity Human Resources (*i.e.*, Workforce) Strategy and identify possible actions within the following areas to help the Federal Government recruit, develop, and maintain a pipeline of cybersecurity talent:

1. **Identify Cybersecurity Workforce Needs**. Improving the government-wide understanding of the cybersecurity workforce by identifying key capability and capacity gaps in order to enhance workforce planning;
2. **Expand the Cybersecurity Workforce through Education and Training.** Working with educational institutions, professional organizations, training organizations, and other experts on cybersecurity program guidance from P-12 through university-level education to significantly expand the pipeline of skilled cybersecurity talent available for the Government and beyond;
3. **Recruit and Hire Highly Skilled Talent**. Engaging in government-wide and agency-specific efforts to expand the cybersecurity workforce through recruitment of highly-skilled talent, and streamlining the hiring and security clearance process while still meeting applicable law and standards; and,
4. **Retain and Develop Highly Skilled Talent**. Promoting an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce.

The Cybersecurity National Action Plan (CNAP), announced on February 9, 2016, builds on the CSIP activities while calling for innovation and investments in cybersecurity education and training to strengthen the talent pipeline. As part of the CNAP, the FY 2017 President's Budget proposes investing $62 million to expand the CyberCorps®: Scholarship for Service program, develop a cybersecurity core curriculum for academic institutions, and strengthen the **National Centers for Academic Excellence in Cybersecurity** Program to increase the number of participating academic institutions and expand cybersecurity education across the Nation. These initiatives will help the Federal Government recruit and retain cybersecurity talent with well-rounded skillsets comprised of the technical acumen, policy expertise, and leadership abilities necessary to secure Federal assets and networks well into the future.

To develop the Strategy, OPM led four teams of representatives from the Government, private sector, and academia to perform a comprehensive review of existing and forward-leaning strategies for recruiting, developing, and retaining cybersecurity professionals. The teams focused on identifying approaches that would help the Federal Government build the cybersecurity workforce and recruit, hire, develop, and retain top talent. OMB and OPM incorporated the findings of the review into the Strategy and considered the following principles

in developing the Strategy:

- Cybersecurity is a shared responsibility among agency leadership, employees, contractors, private industry, and the American people.
- The cybersecurity workforce includes employees who join Federal service at different times in their careers and have different levels of expertise.
- The cybersecurity workforce includes a mix of technical and non-technical professionals focused on all aspects of institutional mission.
- This is a government-wide human capital strategy requiring ownership and action from multiple agencies and entities.
- These initiatives focus primarily on the Federal workforce with the understanding that contractors also play vital roles in Federal cybersecurity.
- The initiatives will provide corresponding resources to non-cyber professionals, such as foundational cybersecurity training and development, and career mobility opportunities.
- While every agency is responsible for managing cybersecurity risks and will have staff that serves part of the cybersecurity workforce, the majority of the civilian cybersecurity workforce will serve in positions at agencies with cybersecurity missions.

I. Identify Cybersecurity Workforce Needs

The Federal Government must adjust its approach for conducting cybersecurity workforce planning. In particular, the Government and Federal agencies should move away from using the term "cyber professionals" as a catchall for the workforce, as the term encompasses over 30 discrete job functions with varying levels of skill and complexity. The National Initiative for Cybersecurity Education (NICE) partner agencies[1] are actively working to address this issue by revising the National Cybersecurity Workforce Framework (Workforce Framework). The Workforce Framework, started in 2011, provides a blueprint for organizing the way we think and talk about cybersecurity work, understanding workforce requirements, and establishing training and development opportunities for employees.

Federal agencies used the Workforce Framework to identify the number of cybersecurity positions and workforce gaps as part of the CSIP review process. Although the CSIP process served as a meaningful first step toward identifying cybersecurity needs, it did not provide a method for agencies to prioritize which position gaps to close. Accordingly, the revised version of the Workforce Framework will enable agencies to examine specific IT, cybersecurity, and cyber-related work roles, and identify personnel skills gaps, rather than merely examining the number of vacancies by job series. Additionally, OPM, the NICE partner agencies, and other Federal agencies are taking the following actions to improve cybersecurity workforce planning:[2]

a. Educate Federal agency Human Resources (HR) and Chief Information Officer (CIO) staff about the Workforce Framework, the tools associated with the Workforce Framework, and the benefits of aligning to the Workforce Framework.
b. Expand cybersecurity position coding to capture work roles outlined in the Workforce Framework, and align those roles with cybersecurity vacancies.
c. Conduct Strategic Workforce Planning, and work with the private sector to explore trends and anticipate future workforce needs.

[1] The NICE partner agencies include the National Institute of Standards and Technology (NIST), DHS, DOD, OPM, Office of the Director of National Intelligence, Department of Commerce, the Department of Education, the National Science Foundation (NSF), the National Security Agency (NSA), Department of Energy, Federal Communications Commission, the Department of Labor, and the Executive Office of the President. For more information, see https://niccs.us-cert.gov/footer/about-national-initiative-cybersecurity-education.

[2] See Appendix A, Goal 1.

II. Expand the Cybersecurity Workforce through Education and Training

There is a critical shortage of cybersecurity talent across the Nation, as the demand for personnel with cyber expertise in both the public and private sectors far exceeds the supply. Within the Federal Government, recruitment and retention challenges and competition from the private sector exacerbate this staff shortage. This results in an increasing demand for cybersecurity professionals who can implement mechanisms for defending systems, networks, and data, and address complex and emerging cyber threats.

The CNAP identified several actions to address workforce challenges and expand the talent pipeline. In particular, the CNAP recognized that long-term investments in nationwide cybersecurity education are crucial to establishing a sustainable cybersecurity workforce. Expanding cybersecurity education will require the Government to stimulate interest in the cyber-related fields through initiatives such as Computer Science for All, which aims to provide all P-12 students access to a rigorous computer science education. The Government must also foster students' academic growth through the development of a flexible cybersecurity core curriculum at institutions of higher education and provide employment opportunities that further develop and apply those skills once students graduate.

In addition to expanding these programs, the Federal Government must take additional steps to expand the pipeline of cybersecurity talent that is available to enter into Federal service. These steps include:

- Collaborating with academic institutions to address skill gaps by identifying or promoting existing foundational curriculum that institutions can consult and adopt; and
- Providing resources to academic institutions to accelerate and expand cybersecurity education across the Nation.

Collaborating with Academic Institutions to Address Skills Gaps through Curriculum

Cybersecurity is a burgeoning academic discipline that encompasses technical and non-technical areas of study with a wide range of complexity. The National Security Agency (NSA) and the Department of Homeland Security (DHS) have designated nearly 200 academic institutions as National Centers of Academic Excellence in Cyber (CAE) based on specified criteria for certain cybersecurity focus areas across the academic disciplines. Each institution in the program develops cybersecurity curricula that align with the specified criteria. While these institutions graduate a broad range of talented students, these students do not always possess a common knowledge base when they enter into Federal service. As a result, agencies are often times spending their limited training funds to close skills gaps and familiarize incoming employees with foundational knowledge, skills, and abilities that universities, colleges, and graduate schools could otherwise teach.

OMB, NSA, and DHS, in coordination with the other NICE partner agencies will collaborate with academic institutions to take the following actions and identify, compile, and disseminate foundational cybersecurity guidelines for academic institutions across the nation to consult and voluntarily adopt:[3]

a. Survey the current state of cybersecurity curriculum with academic partners and other leading institutions to determine common learning outcomes that align cybersecurity education with specific work roles and career paths.
b. Develop cybersecurity curriculum guidelines, knowledge units[4] that provide minimum learning requirements in specific areas, and learning outcomes in partnership with academic organizations.
c. Work with colleges and universities, including minority-serving institutions, to increase recruitment efforts and increase the number of students studying cybersecurity as a profession.

Funding Cybersecurity Higher Education across the Nation

The Government will collaborate with academic institutions to expand cyber education across the Nation through the CAE program. The purpose of the CAE program is to promote higher education in cyber defense and to educate and develop professionals that can address cybersecurity challenges. NSA, in coordination with DHS and the NICE partner agencies, will undertake the following actions to increase the capacity of CAEs, students studying at CAEs, and faculty serving at CAEs:

a. Work with educational organizations to establish financial and professional incentives for cybersecurity experts to serve as faculty at a CAE.[5]
b. Measure the success of supported educational programs such that agencies can document a student's proficiency in the competencies, and knowledge, skills, and abilities associated with each category and Specialty Area in the Workforce Framework.
c. Provide grants to current and prospective CAEs to incentivize academic institutions to enhance the quality of their cybersecurity education programs and expand their programs by increasing capacity to enroll and graduate additional students, teach additional courses, and hire additional faculty.

[3] See Appendix A, Goal 2.

[4] Information on knowledge units is available at https://www.iad.gov/NIETP/documents/Requirements/CAE_IA-CD_KU.pdf.

[5] The CyberCorps® SFS Capacity Track provides funding to increase the number of cybersecurity teachers; curriculum resources; cyber laboratories, test beds and ranges; and professional development.

III. Recruit and Hire Highly-Skilled Cybersecurity Talent

The Government must expand its recruitment campaigns in order to raise awareness of employment opportunities and compete for top cybersecurity talent. Federal agencies can offer prospective cybersecurity employees an opportunity to serve their country in a dynamic work environment that is unlike anywhere else in the public or private sectors. However, the Federal Government struggles to attract and retain cybersecurity talent from both colleges and universities, including the CAEs, and industry.

To overcome these challenges, Federal agencies must engage in strategic recruitment and awareness campaigns, and pursue individuals with cyber talent who, historically, may not have sought out Government careers. Agencies should enhance outreach efforts to reach all segments of society and highlight the ways in which their organizations value diversity and inclusion. Recruiting activities should include outreach to women, who OPM estimates compromise less than 25% of the current cyber workforce. Agencies should sustain their efforts to attract minority students to this work, as OPM estimates that minorities comprise 32% of the cyber workforce compared to 35% of the overall civilian labor force. Additionally, enhancing recruitment efforts will require the Government to dedicate human capital personnel to finding ways to streamline hiring and security clearance processes for cybersecurity personnel consistent with governing law and applicable standards. This effort also includes exploring available authorities or pursuing new authorities to offer prospective employees more competitive compensation and providing meaningful work as part of a clear career path through thoughtful consideration to position descriptions and how grade progressions function.

In an effort to reshape cybersecurity recruitment, the CSIP tasked OPM to provide agencies with information on a number of hiring, pay, and leave flexibilities[6] to help recruit and retain individuals in cybersecurity positions. In addition, OPM issued a memorandum that provided *Guidance on Recruitment, Relocation and Retention Incentives*, which allowed agencies to approve exceptions for certain employees to a calendar year 2010 spending limit on incentives. OPM also held numerous forums and summits with agency CIOs, Chief Human Capital Officers, human capital management professionals, managers with hiring or HR responsibilities, and executives who have responsibility for recruiting and hiring a cybersecurity workforce. These activities helped familiarize agency staff with existing hiring authorities, including direct hire authorities for information security professionals,[7] which will help increase recruitment and hiring efforts across the Government in the near term.

---

[6] Information on hiring, pay, and leave flexibilities is available at: https://www.chcoc.gov/content/Cybersecurity-hiring-pay-and-leave-flexibilities.

[7] Information on direct hire authorities is available at: https://www.opm.gov/policy-data-oversight/hiring-information/direct-hire-authority/#url=Governmentwide-Authority.

OMB, OPM, DHS, and other Federal agencies will take the following actions to enhance outreach, recruitment, hiring, and retention of cybersecurity talent into the Federal Government:[8]

a. In accordance with the CNAP, establish the DHS Cybersecurity Surge Corps, which would dispatch teams of cybersecurity experts to assist agencies with incident response, systems engineering, and enterprise security and policy projects, using a consultant multi-project, multi-skill, multi-disciplinary approach.
b. Develop a Federal Cybersecurity Career Awareness Campaign and Communications Strategy for applicants and agency HR and hiring managers.
c. Establish a cybersecurity HR Cadre, an expert group of HR professionals from across the Government, who will execute a model cybersecurity end-to-end hiring process at agencies that is tailored, timely, and a high quality experience for both applicants and hiring managers.
d. Promote the use of the **PushButtonPD™** that managers, supervisors, and HR Specialists can use to rapidly draft a Federal employee Position Description (PD) leveraging accumulated knowledge in order to streamline position classification.
e. Implement a government-wide recruitment strategy aimed at recruiting diverse talent from among veterans, existing civil service employees, CyberCorps®: Scholarships for Service students, apprenticeship program graduates, and traditional sources. Where possible under existing law, the strategy should also provide opportunities for private sector employees to participate in rotational assignments at Federal agencies, enabling professionals who may be reluctant to commit to a career in Federal service for short periods of time to share their skills with Federal employees while gaining Federal service experience.
f. Examine opportunities to expand mechanisms to bring onboard cybersecurity talent including a cybersecurity track in the Presidential Management Fellows program, exploring direct hire for additional occupations related to cybersecurity, and developing legislation on industry exchange programs and expert and consultants.
g. Establish programs to assist Federal agencies in their use of existing flexibilities for compensation and explore opportunities for new or revised pay programs for cybersecurity positions consistent with other special Federal pay programs (e.g., special salary rates and/or market sensitive pay structures).[9]

[8] See Appendix A, Goal 3.
[9] Information on special salary rates is available at: https://apps.opm.gov/SpecialRates/Index.aspx.

IV. Retain and Develop Highly-Skilled Cybersecurity Talent

In order to retain cybersecurity talent, agencies must foster an environment that provides rewarding and hands-on training experiences; supplies useful and appropriate technology; empowers employees; creates a positive and supportive workplace culture; and acknowledges that some of the cybersecurity employees the Federal Government hopes to attract may only wish to stay for a short period of service. This is a different way of thinking about the Federal workforce and requires new programs, initiatives, and ways of approaching recruitment and retention efforts. Such non-traditional opportunities for training and skills refreshment must be considered in order to retain cybersecurity talent.

Whether employees are entry-level, mid-career, or seasoned executives, developmental and training opportunities are critical to retaining employees. Entry-level staff tend to focus on honing their technical skill sets, gaining access to innovative technology, establishing support and mentoring networks, and gaining meaningful hands-on experience. Mid-career professionals often focus on shaping their career path and advancing their skill sets through job rotations, obtaining certifications, and project management and supervisory experience. Seasoned or executive-level professionals may prioritize making contributions to their domains of expertise within the cybersecurity field, leadership development opportunities, and mentoring the next generation.[10]

An OPM-led team of representatives from the Government, the private sector, and academia performed a comprehensive review of the existing education and talent development opportunities for cybersecurity professionals in the Federal Government, focusing on approaches that will help the Government retain top talent. The team found that while a myriad of talent development opportunities exist, cybersecurity professionals may not be aware of or may not have adequate access to the opportunities. Based on this gap analysis, the team developed a series of findings and recommendations to close these gaps.

Establish an Enterprise-wide Approach to Cybersecurity Employee Retention and Development

An OPM-led team recommended that NIST, the Department of Defense (DOD), and DHS convene to determine what actions are required for each work role with a specific interest on major talent gaps for both Federal employees and contractor employees, in order to fully utilize the existing retention and talent development opportunities. Enterprise-wide workforce planning includes efforts to incorporate certifications and training opportunities so that cybersecurity professionals remain knowledgeable about emerging trends in their area(s) of responsibility, with these and other professional development opportunities serving as retention strategies. In

[10] https://niccs.us-cert.gov/sites/default/files/documents/files/Cybersecurity%20Workforce%20Development%20Toolkit_1.pdf

addition, to strengthen enterprise-wide retention and development efforts, DHS will develop a security-training program for non-cybersecurity employees in occupations and work roles that support the core cybersecurity community. There will also be expanded anti-phishing and other behavior-based training, enabling all Federal employees to possess the requisite knowledge to protect themselves from cyber threats on a daily basis.

OMB, OPM, DHS, and other Federal agencies will take the following actions to promote the most effective cybersecurity talent development and management across the Federal cybersecurity workforce:[11]

a. Increase the focus on retention for top performers by helping agencies develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility.
b. Develop a government-wide cybersecurity orientation program for new cybersecurity professionals.
c. Develop and promote cybersecurity career paths, rotational assignments, and mentoring and coaching programs, to provide employees with opportunities to become subject matter experts in their field or move into managerial roles and take on increased responsibilities.
d. Develop and leverage existing tailored cybersecurity training (e.g., FedVTE) for employees, senior managers, and executives who work in related career fields outside of cybersecurity, including finance and acquisitions, so that budget planning, financial management, and contracting help improve agencies' cybersecurity posture.
e. Develop and leverage existing competitions, certifications, and credentialing to improve the skills of existing employees that may qualify them for potential pay increases or promotions based on demonstrated improvements in technical abilities. Explore a legislative proposal for a cybersecurity skills and education incentive, where employees receive additional compensation based on their demonstrated skills and education.
f. Develop a common training program for specific categories of cybersecurity professionals, including but not limited to those personnel engaged in incident response and penetration testing activities.

[11] See Appendix A, Goal 4.

Conclusion

The Strategy details numerous initiatives that will help strengthen the Federal cybersecurity workforce. We must recognize, however, that these changes will take time to implement. To address cybersecurity challenges in the immediate future, the Administration will invest in the existing Federal workforce through initiatives focused on training and retaining existing talent. At the same time, the Government will adjust the way it recruits talented students and potential employees in the cybersecurity workforce outside Federal service. The long-term success of this Strategy requires concerted attention, innovation, and resources. The initiatives discussed in this Strategy represent a meaningful first step toward engaging Federal and non-Federal stakeholders, and the first step toward providing the resources necessary to establish, strengthen, and grow a pipeline of cybersecurity talent well into the future.

###

APPENDIX A

CYBERSECURITY HUMAN CAPITAL STRATEGY GOAL AND ACTION TRACKER

Goal 1: Identify Cybersecurity Workforce Needs

Purpose Improving the government-wide understanding of the cybersecurity workforce while identifying key capability and capacity gaps in order to enhance workforce planning.

Outcome Improve agencies' understanding of their current cybersecurity workforce to better identify current resource and skill gaps, and improve long-term cybersecurity workforce planning and talent development.

Action	Deadline	Lead Agency/Agencies
Educate Federal agency Human Resources (HR) and Chief Information Officer (CIO) staff about the Workforce Framework, the tools associated with the Workforce Framework, and the benefits of aligning to the Workforce Framework.	3 Months	OPM, NIST, DOD
Expand cybersecurity position coding to capture work roles outlined in the Workforce Framework and aligning those roles with cybersecurity vacancies.	9 Months	OPM, NIST
Conduct Strategic Workforce Planning and work with the private sector to explore trends and anticipate future workforce needs.	12+ Months	All Federal Agencies

Goal 2: Expand the Cybersecurity Workforce through Education and Training

Purpose Collaborate with educational and training organizations to provide guidance on cybersecurity program development.

Outcome Increase awareness of Federal cybersecurity career paths for potential applicants for current vacancies, and develop a pipeline of talent to fill long-term gaps in the cybersecurity workforce.

Action	Deadline	Lead Agency/Agencies
Survey the current state of cybersecurity curriculum with academic partners and other leading institutions to determine common learning	9 Months	NSA, DHS, NIST

outcomes that align cybersecurity education with specific work roles and career paths.		
Work with colleges and universities, including minority-serving institutions, to increase recruitment efforts and increase the number of students studying cybersecurity as a profession.	9 Months	NSA, DHS
Provide grants to current and prospective CAEs to incentivize academic institutions to enhance the quality of their cybersecurity education programs and expand their programs by increasing capacity to enroll and graduate additional students, teach additional courses, and hire additional faculty.	9 Months	NSA
Work with educational organizations to establish financial and professional incentives for cybersecurity experts to serve as faculty at a CAE.	12+ Months	NSA, NICE Partner Agencies
Develop cybersecurity curriculum guidelines, knowledge units that provide minimum learning requirements in specific areas, and learning outcomes in partnership with academic organizations.	12+ Months	NSA, NICE Partner Agencies
Measure the success of supported educational programs such that agencies can document a student's proficiency in the competencies and knowledge, skills, and abilities associated with each category and Specialty Area in the Workforce Framework.	12+ Months	NSA, NICE Partner Agencies

Goal 3: Recruit and Hire Highly Skilled Talent

Purpose Engage in government-wide and agency-specific efforts to conduct outreach and recruitment for cybersecurity talent and improve and expand on existing hiring and retention efforts

Outcome Increase the pipeline of cyber talent entering the Federal workforce, including candidates who have not traditionally considered Federal employment, and provide reliable and effective HR services that enable agencies to immediately fill vacancies.

Action	Deadline	Lead Agency/ Agencies
Promote the use of the PushButtonPD™ that managers, supervisors, and HR Specialists can use to rapidly draft a Federal employee Position Description (PD) leveraging accumulated knowledge in order to streamline position classification.	3 Months	DHS, OPM

Establish the DHS Cybersecurity Surge Corps, which would dispatch teams of cybersecurity experts to assist agencies with incident response, systems engineering and enterprise security, and policy projects, using a consultant multi-project, multi-skill, multi-disciplinary approach.	6 Months	DHS, OPM, OMB, NSF
Establish a cybersecurity HR Cadre, an expert group of HR professionals from across the Government, who will execute a model cybersecurity end-to-end hiring process at agencies that is tailored, timely, and a high quality experience for both applicants and hiring managers.	6 Months	OPM, DHS
Establish programs to assist Federal agencies in their use of existing flexibilities for compensation and explore opportunities for new or revised pay programs for cybersecurity positions consistent with other special Federal pay programs (e.g., special salary rates and/or market sensitive pay structures.	6 Months	OPM
Implement a government-wide recruitment strategy aimed at recruiting diverse talent from among veterans, existing civil service employees, CyberCorps®: Scholarships for Service students, apprenticeship program graduates, and traditional sources. Where possible under existing law, the strategy should also provide opportunities for private sector employees to participate in rotational assignments at Federal agencies, enabling professionals who may be reluctant to commit to a career in Federal service for short periods of time to share their skills with Federal employees while gaining Federal service experience.	6 Months	OPM
Develop a Federal Cybersecurity Career Awareness Campaign and Communications Strategy for applicants and agency HR and hiring managers.	9 Months	OPM, DHS
Examine opportunities to expand mechanisms to bring onboard cybersecurity talent including a cybersecurity track in the Presidential Management Fellows program, exploring direct hire for additional occupations related to cybersecurity, and developing legislation on industry exchange programs and expert and consultants.	12 Months	OPM

Goal 4: Retain and Develop Highly Skilled Talent

Purpose Establish an enterprise-wide approach to retention and development to support the continued enhancement of the cybersecurity workforce and its infrastructure.

Outcome Create a network of cybersecurity professionals to facilitate knowledge sharing, identify potential cybersecurity professionals inside the Federal workforce, and promote long-term professional development through informal and formal channels to improve retention efforts and incentivize greater workforce capabilities.

Action	Deadline	Lead Agency
Increase the focus on retention for top performers by helping agencies develop career paths that leverage existing programs and responsibilities to deliver on best practices of performance management, talent development, and compensation flexibility.	6 Months and Ongoing	OPM
Develop and leverage existing tailored cybersecurity training (e.g. FedVTE) for employees, senior managers, and executives who work in related career fields outside of cybersecurity, including finance and acquisitions so that budget planning, financial management, and contracting help improve agencies' cybersecurity posture.	6 Months	DHS, NIST, DOD
Develop a common training program for specific categories of cybersecurity professionals, including but not limited to those personnel engaged in incident response and penetration testing activities.	6 Months	DHS, OPM
Develop a government-wide cybersecurity orientation program for new cybersecurity professionals.	9 Months	OPM, NIST, DOD, OMB DHS
Develop and leverage existing competitions, certifications, and credentialing to improve the skills of existing employees that may qualify them for potential pay increases or promotions based on demonstrated improvements in technical abilities. Explore a legislative proposal for a cybersecurity skills and education incentive, where employees receive additional compensation based on their demonstrated skills and education.	9 Months	OPM, DOD

Develop and promote cybersecurity career paths, rotational assignments, and mentoring and coaching programs, to provide employees with opportunities to become subject matter experts in their field or move into managerial roles and take on increased responsibilities.	9 Months and Ongoing	OPM, NIST

APPENDIX B

ACRONYMS

Acronym	Definition
CAE	National Centers of Academic Excellence
CIO	Chief Information Officer
CNAP	Cybersecurity National Action Plan
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	Department of Homeland Security
DOD	Department of Defense
HR	Human Resources
IT	Information Technology
NIST	National Institute of Standards of Technology
NSA	National Security Agency
NSF	National Science Foundation
NICE	National Initiative for Cybersecurity Education
OMB	Office of Management and Budget
OPM	Office of Personnel Management
The Strategy	Federal Cybersecurity Workforce Strategy
Workforce Framework	National Cybersecurity Workforce Framework